CLAIMS

What is claimed is:

1. A method for tracking the routing of an electronic document, comprising:

embedding a unique identifier within an electronic document; and

monitoring e-mail messages transmitted from senders to recipients, for detection of e-mail messages having the electronic document embedded therewithin or attached thereto, based on the unique identifier.

2. The method of claim 1 wherein the electronic document is a Microsoft Word document.

3. The method of claim 1 wherein the electronic document is a Microsoft Excel spreadsheet.

4. The method of claim 1 wherein the electronic documents is a Microsoft PowerPoint presentation.

5. The method of claim 1 wherein the electronic document is an Adobe PDF document.

6. The method of claim 1 wherein the electronic document is an HTML document.

7. The method of claim 1 wherein the electronic document is an XML document.

8. The method of claim 1 further comprising logging a recipient of an e-mail message having the electronic document embedded therewithin or attached thereto, in an audit record, when said monitoring detects the e-mail message.

9. The method of claim 8 further comprising logging a sender of an e-mail message having the electronic document embedded therewithin or attached thereto, in an audit record, when said monitoring detects the e-mail message.

10. The method of claim 9 further comprising logging a date and time of transmission of an e-mail message having the electronic document embedded therewithin or attached thereto, in an audit record, when said monitoring detects the e-mail message.

11. The method of claim 10 further comprising generating a tracking report from audit records, corresponding to at least one specified document.

12. The method of claim 10 further comprising generating a tracking report from audit records, corresponding to at least one specified user.

13. The method of claim 10 further comprising generating a tracking report from the audit records, corresponding to a specified time period.

14. The method of claim 1 further comprising logging the most recent file name of a file storing the electronic document, in an audit record, when said monitoring detects an e-mail message having the electronic document embedded therewithin or attached thereto.

15. The method of claim 1 wherein said monitoring comprises authenticating the unique identifier.

16. The method of claim 15 further comprising issuing a notification if said authenticating fails to authenticate the unique identifier.

17. The method of claim 1 further comprising:

examining an access control policy to determine whether or not permission is granted to transmit the electronic document to a recipient of an e-mail message having the electronic document embedded therewithin or attached thereto; and

causing transmission of the e-mail message to the recipient to be blocked, if said examining determines that permission is not granted.

18. The method of claim 17 further comprising issuing a notification about said causing to be blocked.

19. A system for tracking the routing of an electronic document, comprising:

an auto-marker for embedding a unique identifier within an electronic document; and

a traffic monitor for monitoring e-mail messages transmitted from senders to recipients, and for detecting e-mail messages having the electronic document embedded therewithin or attached thereto, based on the unique identifier.

20. The system of claim 19 wherein the electronic document is a Microsoft Word document.

21. The system of claim 19 wherein the electronic document is a Microsoft Excel spreadsheet.

22. The system of claim 19 wherein the electronic document is a Microsoft PowerPoint presentation.

23. The system of claim 19 wherein the electronic document is an Adobe PDF document.

24. The system of claim 19 wherein the electronic document is an HTML document.

25. The system of claim 19 wherein the electronic document is an XML document.

26. The system of claim 19 further comprising an auditor for logging a recipient of an e-mail message having the electronic document embedded therewithin or attached thereto, in an audit record, when said traffic monitor detects the e-mail message.

27. The system of claim 26 further comprising an auditor for logging a sender of an e-mail message having the electronic document embedded therewithin or attached thereto, in an audit record, when said traffic monitor detects the e-mail message.

28. The system of claim 27 further comprising an auditor for logging a date and time of transmission of an e-mail message having the electronic document embedded therewithin or attached thereto, in an audit record, when said traffic monitor detects the e-mail message

29. The system of claim 28 further comprising a reporter for generating a tracking report from audit records, corresponding to at least one specified document.

30. The system of claim 28 further comprising a reporter for generating a tracking report from audit records, corresponding to at least one specified user.

31. The system of claim 28 further comprising a reporter for generating a tracking report from audit records, corresponding to a specified time period.

32. The system of claim 19 further comprising an auditor for logging the most recent file name of a file storing the electronic document, in an audit record, when said traffic monitor detects an e-mail message having the electronic document embedded therewithin or attached thereto.

33. The system of claim 19 further comprising a scanner for authenticating the unique identifier.

34. The system of claim 33 further comprising a notifier for issuing a notification if said authenticating fails to authenticate the unique identifier.

35. The system of claim 19 further comprising:

a policy manager for examining an access control policy to determine whether or not permission is granted to transmit the electronic document to a recipient of an e-mail message having the electronic document embedded therewithin or attached thereto; and

a policy enforcer for causing transmission of the e-mail message to the recipient to be blocked, if said policy manager determines that permission is not granted.

36. The system of claim 35 further comprising a notifier for issuing a notification about said policy enforcer causing transmission of the e-mail message to be blocked.

37. A computer-readable storage medium storing program code for causing a computer to perform the steps of:

embedding a unique identifier within an electronic document; and

monitoring e-mail messages transmitted from senders to recipients, for detection of the electronic document embedded therewithin or attached thereto, based on the unique identifier.

38. A method for tracking the routing of an electronic document, comprising:

embedding a unique identifier within an electronic document; and

monitoring transmitted network packets, for detection of network packets containing the electronic document, based on the unique identifier.

39. The method of claim 38 further comprising logging an audit record of the transmission, when a network packet containing the electronic document is detected by said monitoring.

40. The method of claim 39 wherein said logging includes logging a date and time of the transmission in the audit record.

41. The method of claim 39 wherein said logging includes logging a destination of the transmission in the audit record.

42. The method of claim 38 wherein said monitoring monitors networks packets transmitted internally within an organization network.

43. The method of claim 38 wherein said monitoring monitors networks packets transmitted from within an organization network to outside of the organization network.

44. The method of claim 38 wherein said monitoring monitors networks packets transmitted to an organization network from outside of the organization network.

45. The method of claim 38 wherein the network packets are transmitted in response to an FTP download.

46. The method of claim 38 wherein the network packets are transmitted in response to an HTTP download.

47. The method of claim 38 wherein the network packets are transmitted in response to an Instant Messenger download.

48. A system for tracking the routing of an electronic document, comprising:

an auto-marker for embedding a unique identifier within an electronic document; and

a traffic monitor for monitoring transmitted network packets, and for detection of network packets containing the electronic document, based on the unique identifier.

49. The system of claim 48 further comprising an auditor for logging an audit record of the transmission when a network packet containing the electronic document is detected by said traffic monitor.

50. The system of claim 49 wherein said auditor logs a date and time of the transmission in the audit record.

51. The system of claim 49 wherein said auditor logs a destination of the transmission in the audit record.

52. The system of claim 48 wherein said traffic monitor monitors networks packets transmitted internally within an organization network.

53. The system of claim 48 wherein said traffic monitor monitors networks packets transmitted from within an organization network to outside of the organization network.

54. The system of claim 48 wherein said traffic monitor monitors networks packets transmitted to an organization network from outside of the organization network.

55. The system of claim 48 wherein the network packets are transmitted in response to an FTP download.

56. The system of claim 48 wherein the network packets are transmitted in response to an HTTP download.

57. The system of claim 48 wherein the network packets are transmitted in response to an Instant Messenger download.

58. A computer-readable storage medium storing program code for causing a computer to perform the steps of:

embedding a unique identifier within an electronic document; and

monitoring transmitted network packets, for detection of network packets containing the electronic document, based on the unique identifier.

59. A method for controlling distribution of an electronic document within computer networks, comprising:

intercepting e-mail messages being transmitted from senders to recipients;

scanning the intercepted e-mail messages for detection of a specified electronic document embedded therein or attached thereto;

examining a policy to determine whether or not transmission of the document to a recipient is permitted, if said scanning detects an e-mail message having the electronic document embedded therein or attached thereto; and

causing transmission of the document to the recipient to be blocked, if said examining determines that transmission is not permitted.

60. The method of claim 59 wherein said scanning detects the electronic document based on a unique identifier embedded therewithin.

61. The method of claim 59 wherein the policy indicates recipients permitted to access the electronic document.

62. The method of claim 59 wherein the policy indicates recipients not permitted to access the electronic document.

63. The method of claim 59 wherein the policy indicates senders permitted to send the electronic document.

64. The method of claim 59 wherein the policy indicates senders not permitted to send the electronic document.

65. The method of claim 59 further comprising issuing a notification, if said examining determines that transmission is not permitted.

66. The method of claim 59 further comprising generating an audit record to record transmission of the electronic document via an e-mail message, if said examining determines that transmission is permitted.

67. A system for controlling distribution of an electronic document within computer networks, comprising:

a traffic monitor for intercepting e-mail messages being transmitted from senders to recipients;

a scanner for scanning the intercepted e-mail messages, and for detecting a specified electronic document embedded therein or attached thereto;

a policy manager for examining a policy to determine whether or not transmission of the document to a recipient of an e-mail message is permitted; and

a policy enforcer for causing transmission of the document to the recipient to be blocked.

68. The system of claim 67 wherein said scanner detects the electronic document based on a unique identifier embedded therewithin.

69. The system of claim 67 wherein the policy indicates recipients permitted to access the electronic document.

70. The system of claim 67 wherein the policy indicates recipients not permitted to access the electronic document.

71. The system of claim 67 wherein the policy indicates senders permitted to send the electronic document.

72. The system of claim 67 wherein the policy indicates senders not permitted to send the electronic document.

73. The system of claim 67 further comprising a notifier for issuing a notification, if said examining determines that transmission is not permitted.

74. The system of claim 67 further comprising an auditor for generating an audit record, to record transmission of the electronic document via an e-mail message, if said policy manager determines that transmission is permitted.

75. A computer-readable storage medium storing program code for causing a computer to perform the steps of:

intercepting e-mail messages being transmitted from senders to recipients;

scanning the intercepted e-mail messages for detection of a specified electronic document embedded therein or attached thereto;

examining a policy to determine whether or not transmission of the document to a recipient is permitted, if said scanning detects an e-mail message having the electronic document embedded therein or attached thereto; and

causing transmission of the document to the recipient to be blocked, if said examining determines that transmission is not permitted.

76. A method for controlling distribution of an electronic document within computer networks, comprising:

intercepting network packets transmitted over a computer network;

scanning the intercepted network packets for detection of network packets containing a specified electronic document;

examining a policy to determine whether or not transmission of the specified electronic document is permitted, if said scanning detects a network packet containing the specified electronic document; and

causing transmission of the document to be blocked, if said examining determines that transmission is not permitted.

77. The method of claim 76 wherein said scanning detects the specified electronic document based on a unique identifier embedded therewithin.

78. The method of claim 76 wherein the policy indicates recipients permitted to access the specified electronic document.

79. The method of claim 76 wherein the policy indicates recipients not permitted to access the specified electronic document.

80. The method of claim 76 wherein the network packets are transmitted in response to an FTP download.

81. The method of claim 76 wherein the network packets are transmitted in response to an HTTP download.

82. The method of claim 76 wherein the network packets are transmitted in response to an Instant Messenger download.

83. A system for controlling distribution of an electronic document within computer networks, comprising:

a traffic monitor for intercepting network packets transmitted over a computer network;

a scanner for scanning the intercepted network packets and for detecting network packets containing a specified electronic document;

a policy manager for examining a policy to determine whether or not transmission of the specified electronic document is permitted; and

a policy enforcer for causing transmission of the document to be blocked.

84. The system of claim 83 wherein said scanner detects the specified electronic document based on a unique identifier embedded therewithin.

85. The system of claim 83 wherein the policy indicates recipients permitted to access the specified electronic document.

86. The system of claim 83 wherein the policy indicates recipients not permitted to access the specified electronic document.

87. The system of claim 83 wherein the network packets are transmitted in response to an FTP download.

88. The system of claim 83 wherein the network packets are transmitted in response to an HTTP download.

89. The system of claim 83 wherein the network packets are transmitted in response to an Instant Messenger download.

90. A computer-readable storage medium storing program code for causing a computer to perform the steps of:

intercepting network packets transmitted over a computer network;

scanning the intercepted network packets for detection of network packets containing a specified electronic document;

examining a policy to determine whether or not transmission of the specified electronic document is permitted, if said scanning detects a network packet containing the specified electronic document; and

causing transmission of the document to be blocked, if said examining determines that transmission is not permitted.